Avaya Solution & Interoperability Test Lab

Application Notes for Configuring @Comm CommView CPE with Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required to allow @Comm CommView CPE to collect call detail records from Avaya Communication Manager using Avaya Reliable Session Protocol over TCP/IP. The CommView CPE collects, stores and processes these call records to provide usage analysis, call costing and billing capabilities.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describes a compliance-tested call detail recording (CDR) solution comprised of Avaya Communication Manager and @Comm CommView CPE. The CommView CPE is a call accounting software application that uses call detail records to provide reporting capabilities to business and IT managers to track and manage call usage and telecom expenses.

Avaya Communication Manager communicates to @Comm CommView CPE via an Avaya Reliable Session Protocol (RSP) session over the TCP/IP network. The RSP session provides a transport mechanism for reliable delivery of CDR records. Avaya Communication Manager generates and sends the call records out on the RSP session while the CommView CPE collects, stores and processes the records at the other end.

The CommView CPE is comprised of two components that reside on a Windows PC at the customer's premises: the CommView Avaya Server application and the CommView main application. The CommView Avaya Server application runs as a background service process that terminates the RSP protocol, collects the call records from Avaya Communication Manager, and stores the records in a text file. The CommView main application periodically pulls the data from the text file, parses the data and places the information in a database. The database is then used to provide the reporting capabilities.

Avaya Communication Manager can generate call detail records for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conference calls. The CommView CPE can support any CDR format provided by Avaya Communication Manager. As part of the CommView CPE product registration process, @Comm technical support creates a custom PBX configuration file to accurately parse the CDR data. For the compliance testing, the expanded format was utilized.

Figure 1 illustrates a sample configuration that was used for the compliance test. The configuration consists of three Avaya Media Servers running Avaya Communication Manager. Site A is comprised of Avaya Communication Manager runs on an Avaya S8700 Servers with an Avaya G650 Media Gateway. Site B is comprised of Avaya Communication Manager runs on an Avaya S8300 Server residing in an Avaya G700 Media Gateway. Each Avaya Communication Manager is connected to an IP network comprised of an Extreme Networks Summit 48 layer 3 switch. @Comm CommView CPE running on a Windows 2000 PC is connected to the IP network at site A and has a RSP session established to each Avaya Communication Manager to collect CDR records. Each system has trunks and phones associated with it to generate calls. Avaya 4600 Series IP Telephones, Avaya 9600 Series IP Telephones, and Avaya 6400D Series Digital Telephones are registered to both Avaya S8700 and S8300 Servers. In addition, there is an H.323 IP trunk established between the two media servers.

Site C is comprised of an Avaya S8300 Server with an Avaya G350 Media Gateway, which has connections to an Avaya 4600 Series IP Telephone and Avaya 6400D Series Digital Telephone.

The Avaya S8300 Server, installed with Local Survivable Processor (LSP) license, is setup as a LSP to Site A.

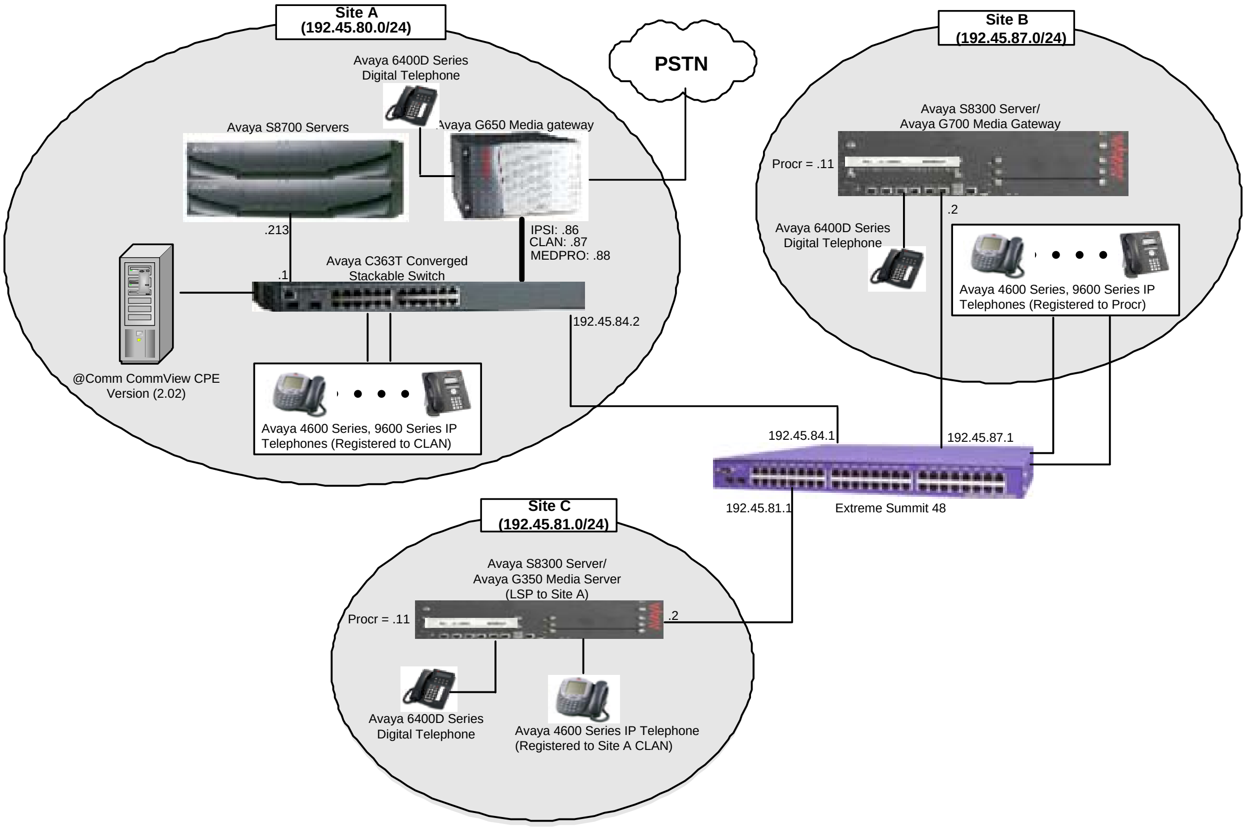


Figure 1: Test configuration: Commview collecting CDR data from multiple Avaya Servers

2. Equipment and Software Validated

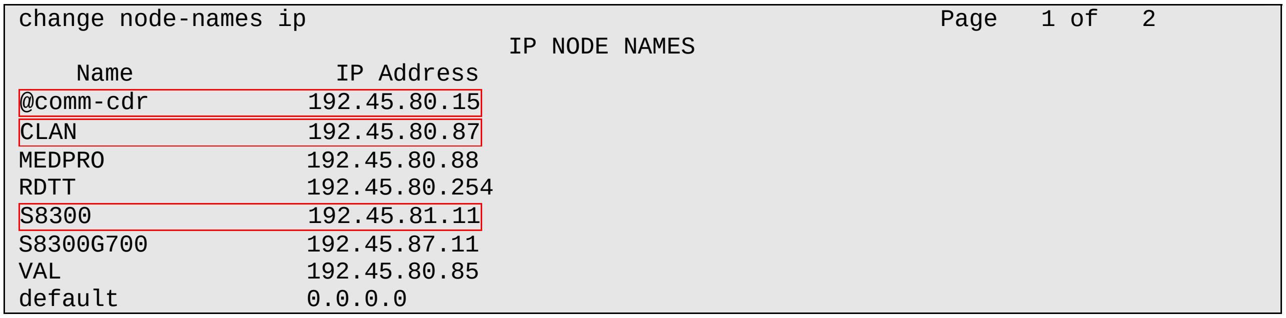
The following equipment and software/firmware were used for the test configuration provided.

Equipment		Software/Firmware
Avaya S8700 Servers		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface TN799DP CLAN Interface TN2302AP IP Media Processor TN2602AP IP Media Processor	HW11 FW030 HW01 FW017 HW20 FW108 HW02 FW007
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya S8300 Server with Avaya G350 Media Gateway (with LSP license)		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya 4600 Series IP Telephones		
	4620 (H.323) 4625 (H.323)	2.8 2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6400D Series Digital Telephones		-
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Networks Summit 48		4.1.21
@Comm CommView CPE		2.02

3. Configure Avaya Communication Manager

This section describes the procedure for configuring call detail recording (CDR) in Avaya Communication Manager. These steps are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8700 Server. All steps are the same for the other Avaya Servers unless otherwise noted. Avaya Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the PC running the CommView CPE. For the Avaya S8700 Server, the RSP link originates at the IP address of the CLAN board. For the Avaya S8300 Media Server, the RSP link originates at the IP address of the local processor (with node-name – “procr”).

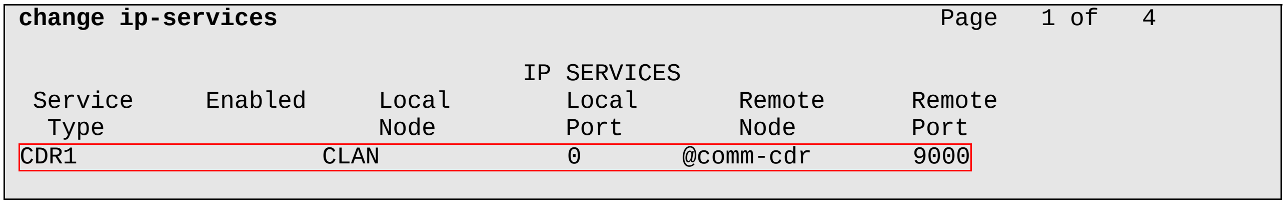
Use the **change node-names ip** command to create a new node name, for example, **@comm-cdr**. This node name is associated with the IP Address of the PC running the CommView CPE application. Also, take note of the node name – "CLAN". It will be used in the next step. The CLAN entry on this form was previously administered. S8300 is an LSP licensed Avaya S8300 Server.



```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
@comm-cdr              192.45.80.15
CLAN                   192.45.80.87
MEDPRO                 192.45.80.88
RDTT                   192.45.80.254
S8300                  192.45.81.11
S8300G700              192.45.87.11
VAL                    192.45.80.85
default                0.0.0.0
```

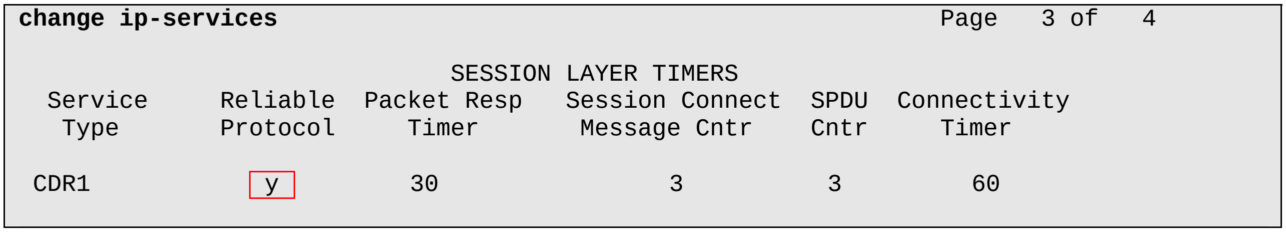
Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, provide the following information:

- Service Type: **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- Local Node: **CLAN** [For the Avaya S8700 Server, the Local Node is set to the node name of the CLAN board. If the Avaya S8300 Server was utilized, set the Local Node to **procr**.]
- Local Port: **0** [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.]
- Remote Node: **@comm-cdr** [The Remote Node is set to the node name previously defined.]
- Remote Port: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in the CommView CPE.]



```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
CDR1                    CLAN            0        @comm-cdr        9000
```

On Page 3 of the ip-services form, enable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to **y**.



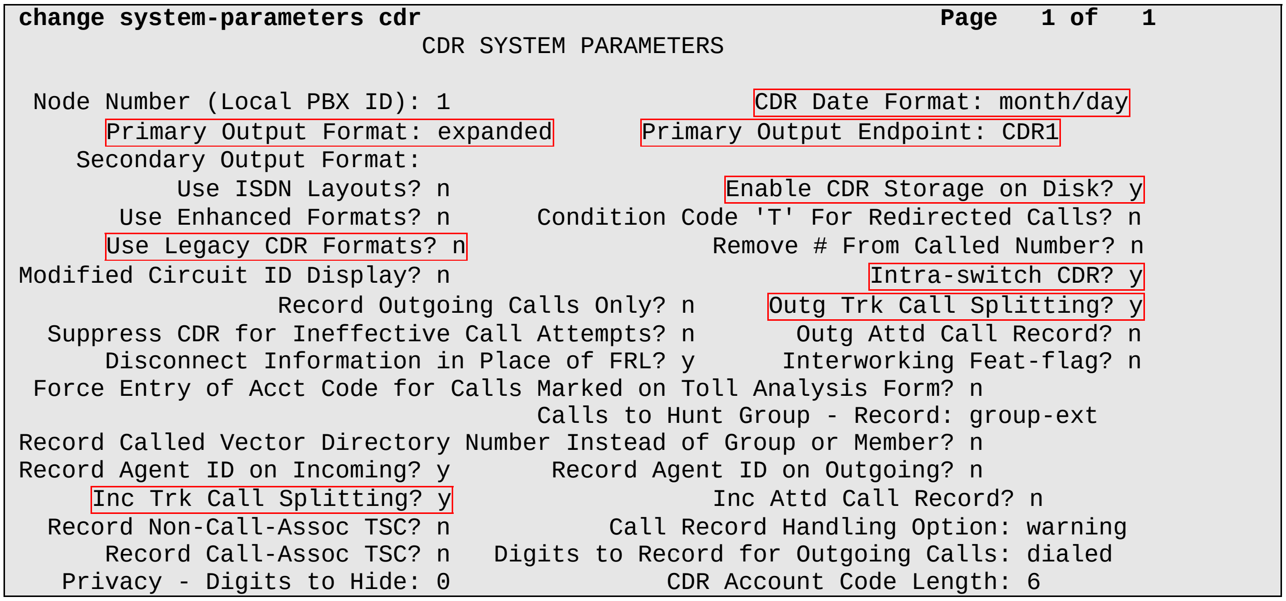
```
change ip-services                                              Page   3 of   4

                              SESSION LAYER TIMERS
  Service      Reliable  Packet Resp  Session Connect  SPDU  Connectivity
   Type        Protocol     Timer      Message Cntr    Cntr     Timer

 CDR1             y          30                 3         3         60
```

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- CDR Date Format: **month/day**
- Primary Output Format: **expanded**
- Primary Output Endpoint: **CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- Enable CDR Storage on Disk?: **y** [Enable the Survivable CDR feature. Default is **n**.]
- Use Legacy CDR Formats?: **n** [Allows CDR formats to use 4.x CDR formats. If the field is set to **y**, then CDR formats utilize the 3.x CDR formats.]
- Intra-switch CDR: **y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH CDR form.]
- Record Outgoing Calls Only?: **n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- Outg Trk Call Splitting?: **y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- Inc Trk Call Splitting?: **y** [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]



```
change system-parameters cdr                                    Page   1 of   1
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                      CDR Date Format: month/day
      Primary Output Format: expanded      Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? n                 Remove # From Called Number? n
Modified Circuit ID Display? n                             Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? n       Outg Attd Call Record? n
      Disconnect Information in Place of FRL? y      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: group-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y       Record Agent ID on Outgoing? n
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 6
```

If the Intra-switch CDR field is set to **y** on Page 1 of the system-parameters cdr form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked. To simplify the process of adding multiple extensions in the Assigned Members field, the “Intra-switch CDR by COS” feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

```
change intra-switch-cdr                                        Page   1 of   2
                           INTRA-SWITCH CDR

Assigned Members:   4    of 5000   administered
  1: 22001     19:          37:          55:          73:          91:
  2: 22002     20:          38:          56:          74:          92:
  3: 22003     21:          39:          57:          75:          93:
  4: 22007     22:          40:          58:          76:          94:
  5:           23:          41:          59:          77:          95:
  6:           24:          42:          60:          78:          96:
  7:           25:          43:          61:          79:          97:
```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the CDR Reports field is set to **y**. This applies to all types of trunk groups.

```
change trunk-group 80                                          Page   1 of  20
                                TRUNK GROUP

Group Number: 80                  Group Type: isdn          CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 1        TAC: 103
   Direction: two-way        Outgoing Display? y        Carrier Medium: PRI/BRI
 Dial Access? y                Busy Threshold: 255      Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                   Digital Loss Group: 13
Incoming Calling Number - Delete:     Insert:                Format:
              Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? y
 Answer Supervision Timeout: 0
```

Repeat above steps for the Avaya S8300 Server running Avaya Communication Manager. The CDR format and port number used for the CDR link must be the same for each Avaya Communication Manager sending CDR records to the CommView CPE.

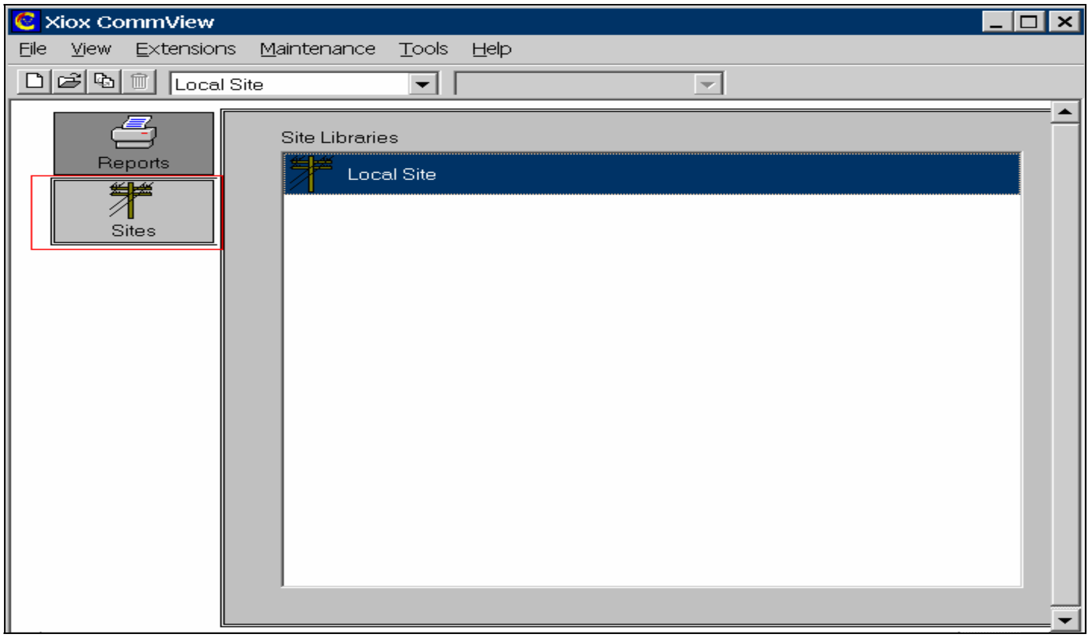
4. Configure @Comm CommView CPE

This section describes the configuration of @Comm CommView CPE. It is comprised of two components: CommView Avaya Server and the CommView main application. Each component is installed and configured separately. For installation procedures, please refer to the CommView CPE Installation Guide [3].

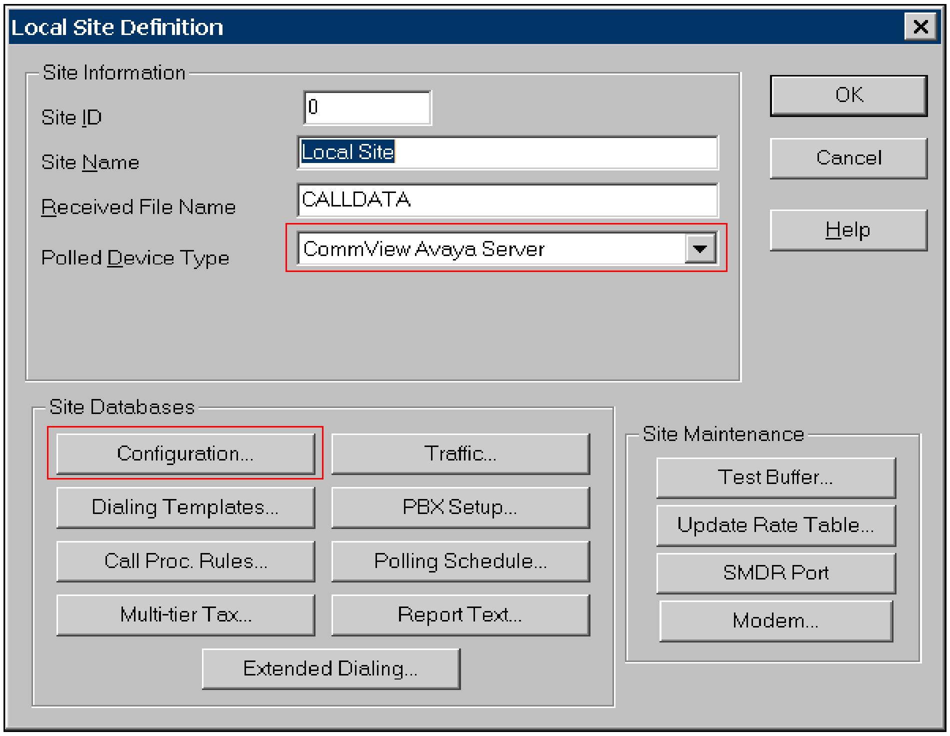
4.1. CommView Main Application

This section describes how to configure the main application for processing CDR records from Avaya Communication Manager. Perform the CommView main application installation procedures outlined in the @Comm CommView CPE documentation. If multiple sites are included in the configuration, then each site requires a separate license to be purchased from @Comm before the configuration of the additional sites can be performed as shown in the following procedure.

Launch the CommView main application from the Microsoft Windows Start menu by navigating to **Start →Programs → CommView → CommView**. To begin configuration of a particular site, select the **Sites** icon on the left-hand side of the main window. When the Site Libraries list appears, highlight the name of the site to be configured as shown below. By default, there is always one site called Local Site. If additional site licenses have been purchased from @Comm, then additional sites can be added. The Local Site in the test configuration was the Avaya S8700 Server running Avaya Communication Manager. Double click **Local Site**.



In the Local Site Definition window, select **CommView Avaya Server** for the Polled Device Type field. Select the **Configuration** button to provide additional information.



Local Site Definition

Site Information

Site ID: 0

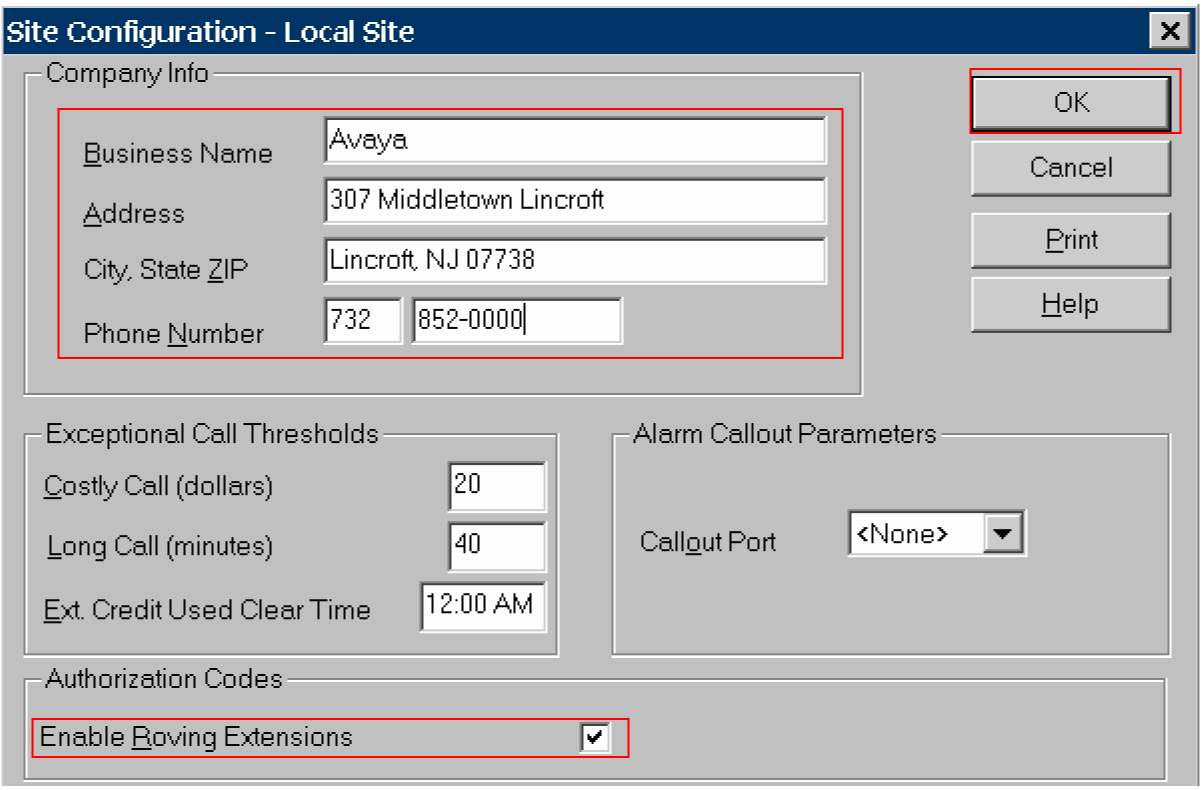
Site Name: Local Site

Received File Name: CALLDATA

Polled Device Type: CommView Avaya Server

Fill in all data in the Company Info portion of the screen. The Phone Number is important because it is used for determining which calls are local to this site and calculating call rates. If this site uses authorization codes, then the box next to **Enable Roving Extensions** at the bottom of the screen must be checked. Leave the default values for all other fields.

Select **OK** to submit the data.



Site Configuration - Local Site

Company Info

Business Name: Avaya

Address: 307 Middletown Lincroft

City, State ZIP: Lincroft, NJ 07738

Phone Number: 732 852-0000

Exceptional Call Thresholds

Costly Call (dollars): 20

Long Call (minutes): 40

Ext. Credit Used Clear Time: 12:00 AM

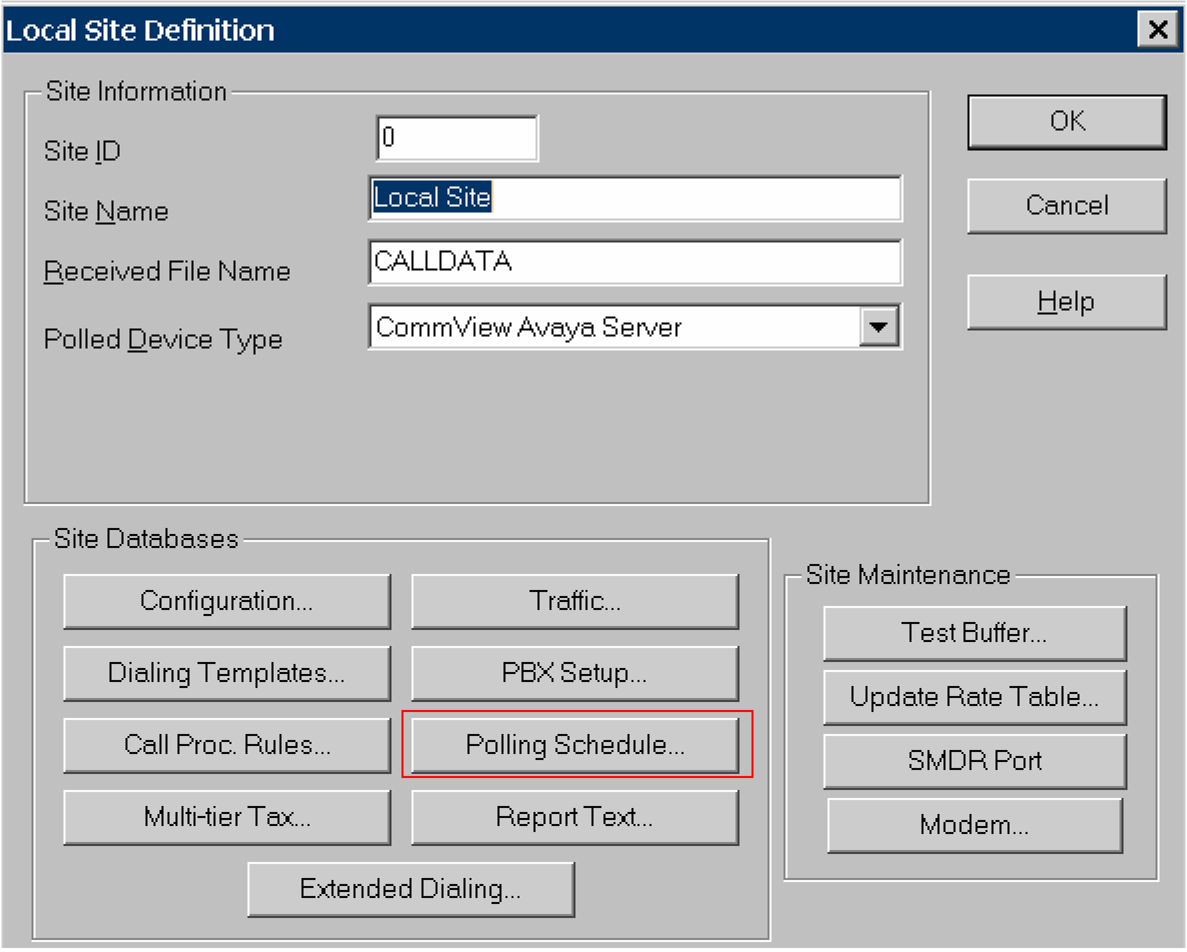
Alarm Callout Parameters

Callout Port: <None>

Authorization Codes

Enable Roving Extensions ☑

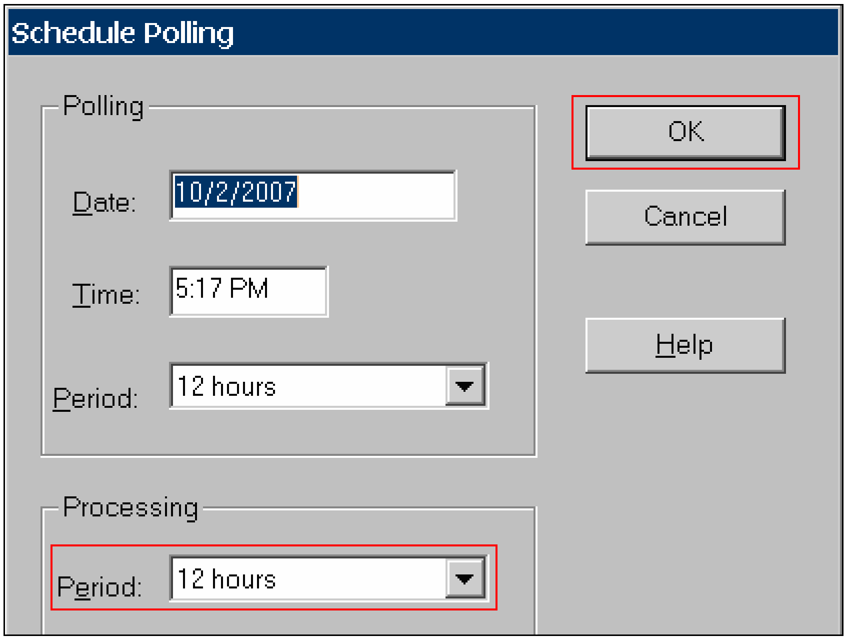
The rate at which data is pulled from CommView Avaya Server and processed by the CommView main application can be changed by altering the polling schedule. The default schedule will be sufficient in most cases. If the user wishes to alter the default values, select the **Polling Schedule** button in the Local Site Definition window.



Site ID: 0
Site Name: Local Site
Received File Name: CALLDATA
Polled Device Type: CommView Avaya Server

Enter the desired interval in the Processing Period field. The Polling Period is not used for connections to Avaya Communication Manager since Avaya Communication Manager pushes the data to the receiving application. The example below shows the default values. For the purposes of the testing, the Processing Period was set to a much smaller interval than shown below to reduce the time waiting for records to be processed.

Select **OK** to submit the data.



Schedule Polling

Polling

Date: 10/2/2007

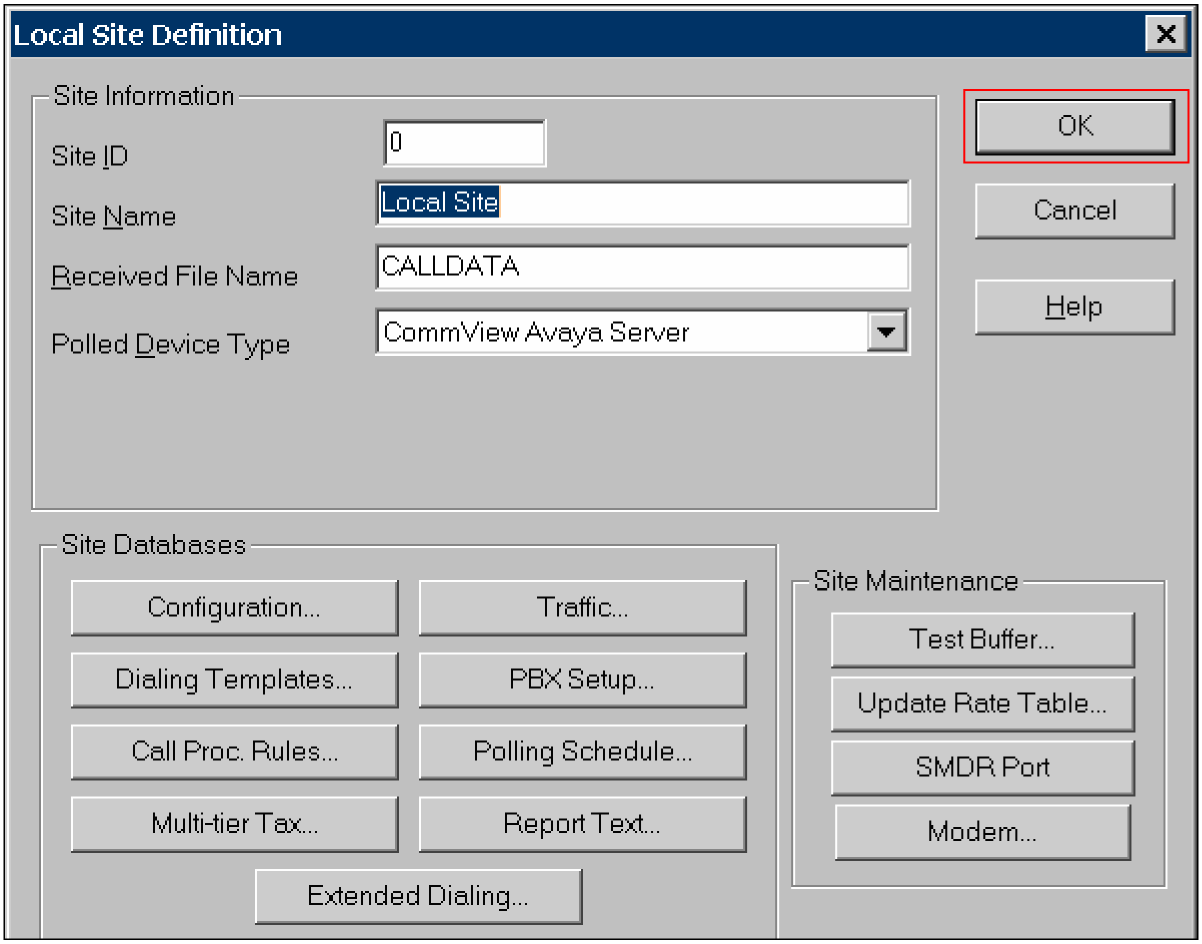
Time: 5:17 PM

Period: 12 hours

Processing

Period: 12 hours

Select **OK** to submit the data collected in the previous steps. Note that selecting PBX Setup from the Local Site Definition window was not required. This part of the configuration was done earlier by @Comm technical support as part of the installation and product registration process.



Local Site Definition

Site Information

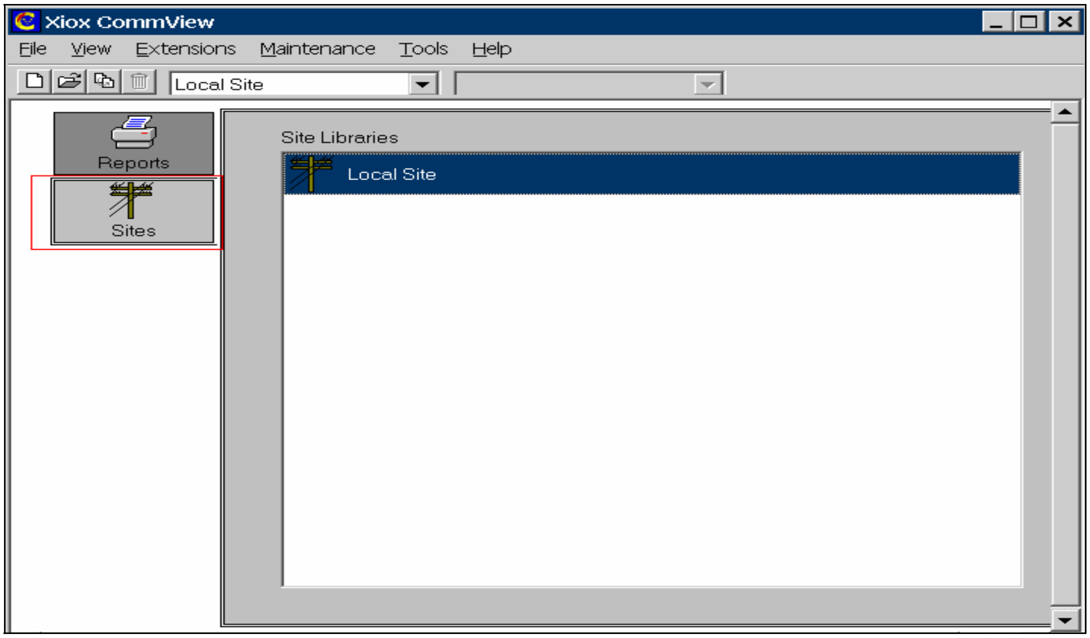
Site ID: 0

Site Name: Local Site

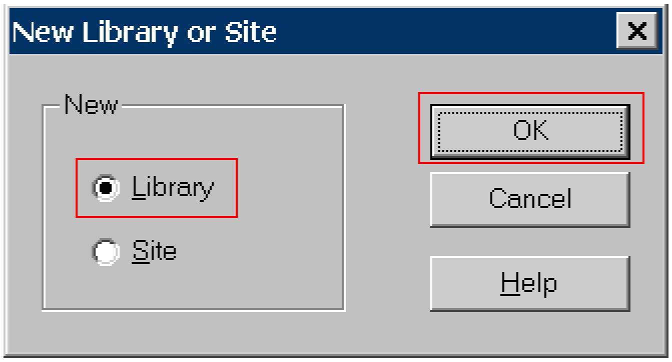
Received File Name: CALLDATA

Polled Device Type: CommView Avaya Server

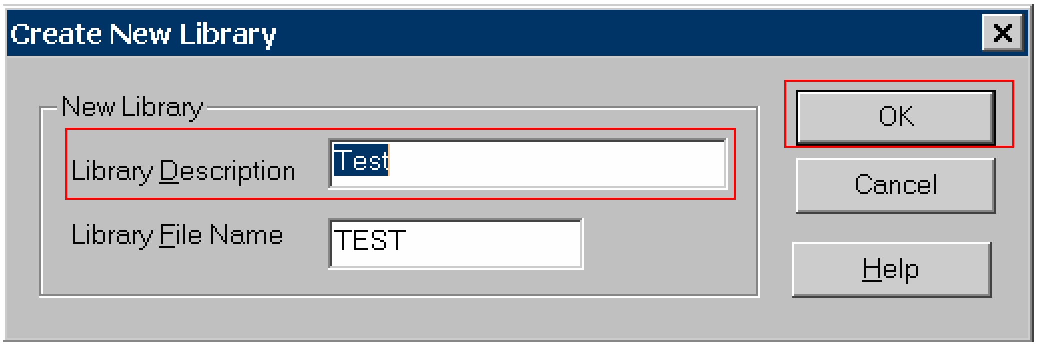
To add a second site, the user must first create a directory (or library) to hold the information for the site(s). To accomplish this task, select the **Sites** icon and then navigate to **File → New** from the screen below.



Select **Library** and then click **OK**.



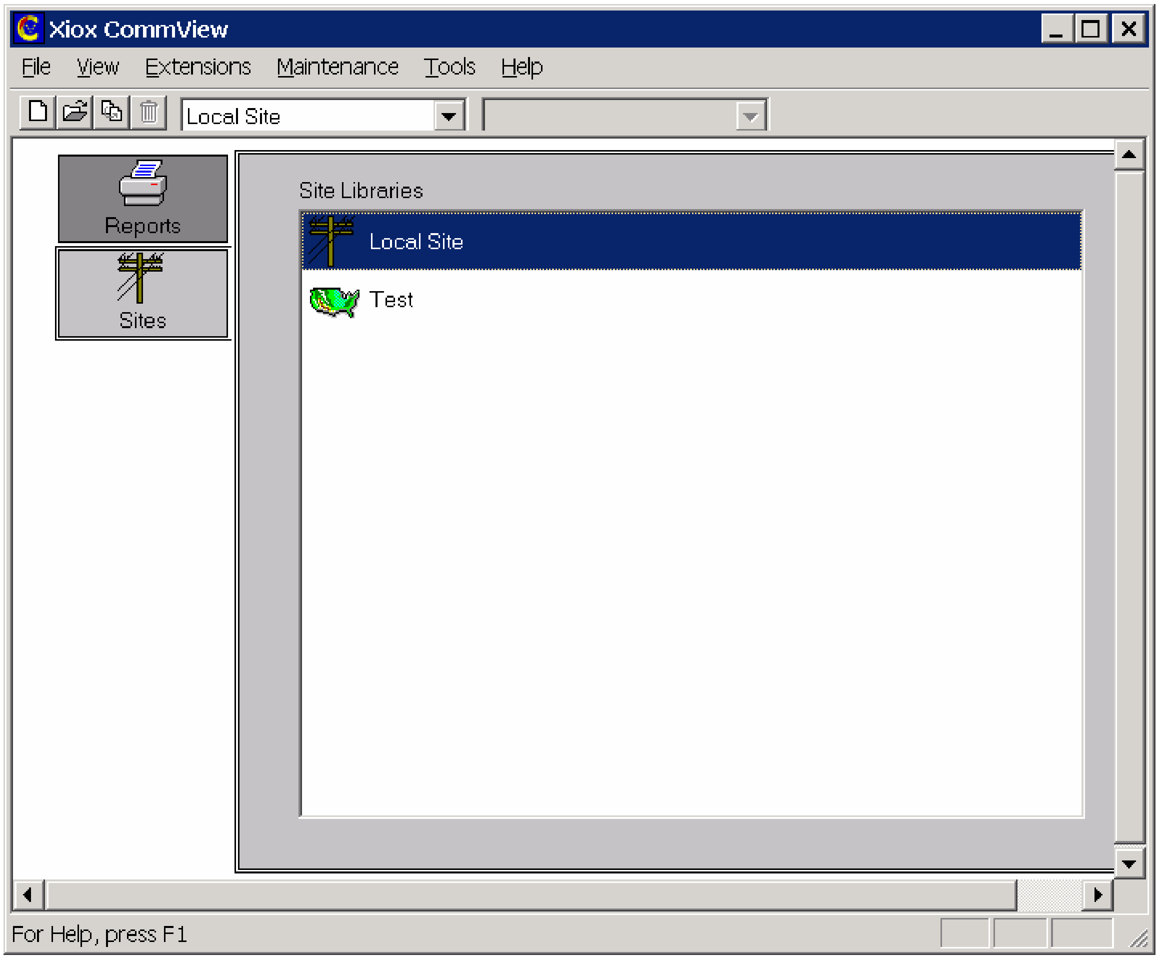
Enter a short description and name for the library. Click **OK**.



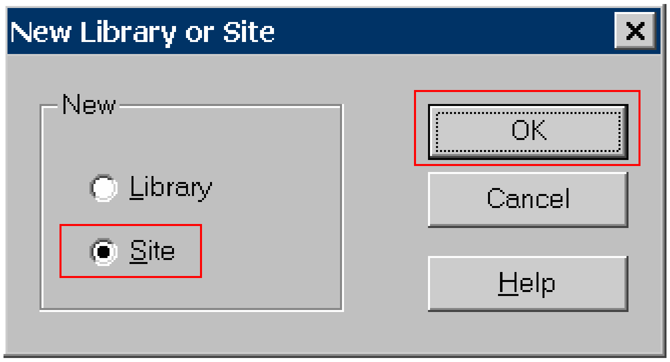
Library Description: Test

Library File Name: TEST

After the library is created, again navigate to **File → New** from the screen below to create the site in the new library. In the test configuration, the remote site was the Avaya S8300 Server.



Select **Site** and then click **OK**.

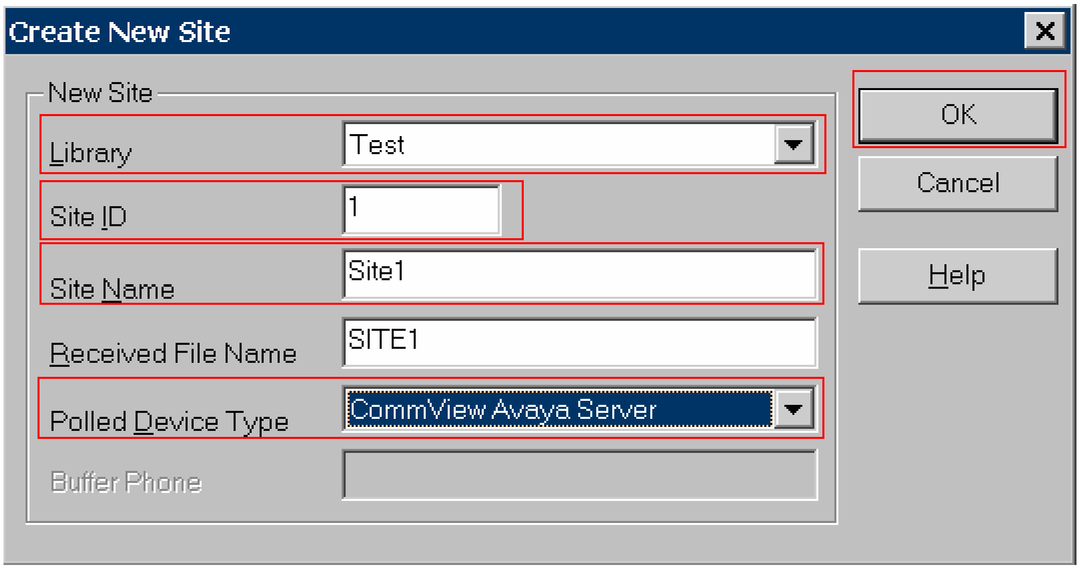

New Library or Site

New

○ Library

● Site

From the Library pulldown menu, select the library description entered when the library was created. Use the default value for Site ID. Site Name can be any arbitrary name. From the Polled Device Type pulldown menu, select **CommView Avaya Server**.
Select **OK**.


Create New Site

New Site

Library: Test

Site ID: 1

Site Name: Site1

Received File Name: SITE1

Polled Device Type: CommView Avaya Server

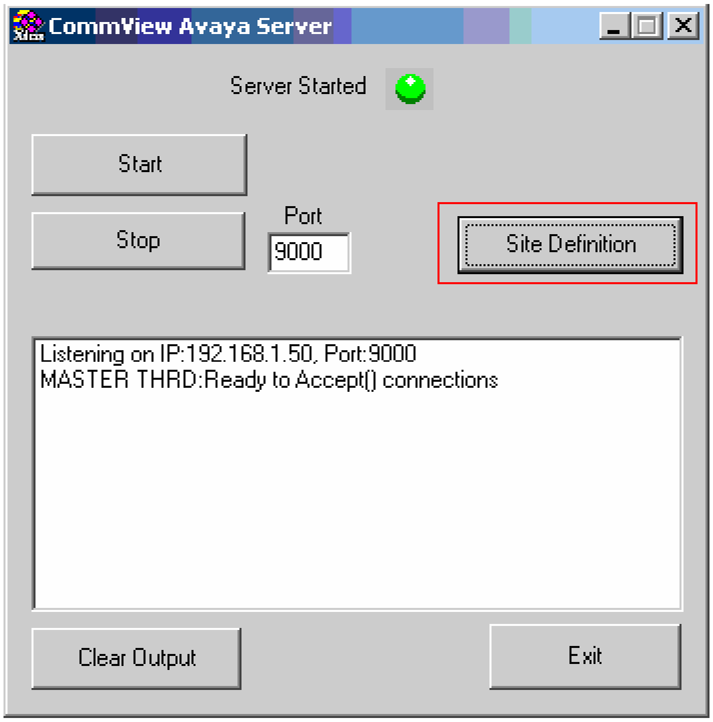
Buffer Phone:

4.2. CommView Avaya Server Application

This section describes the configuration steps for the CommView Avaya Server component of the CommView CPE.

Perform the CommView Avaya Server installation procedures outlined in the @Comm CommView CPE documentation. CommView Avaya Server is installed as a service under Microsoft Windows that will start automatically. When CommView Avaya Server starts running, the following window is displayed.

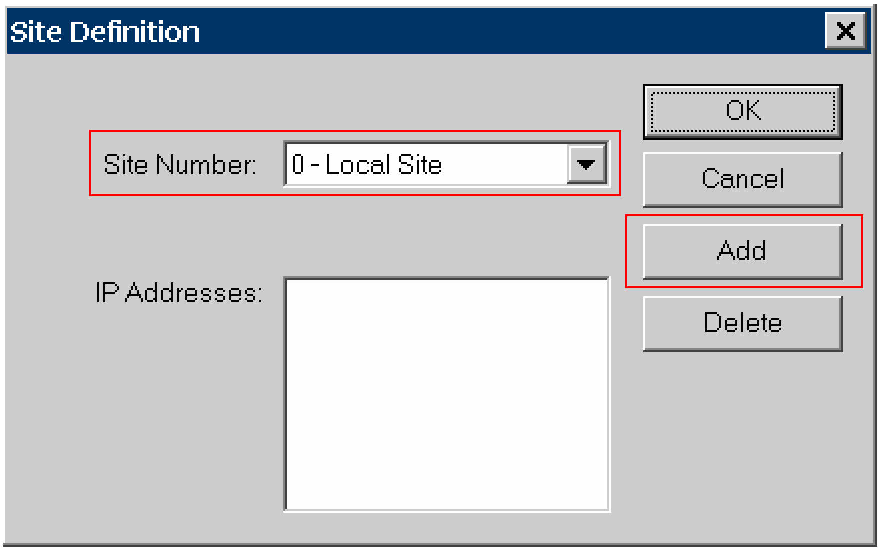
To begin configuration, select the **Site Definition** button.



Port: 9000

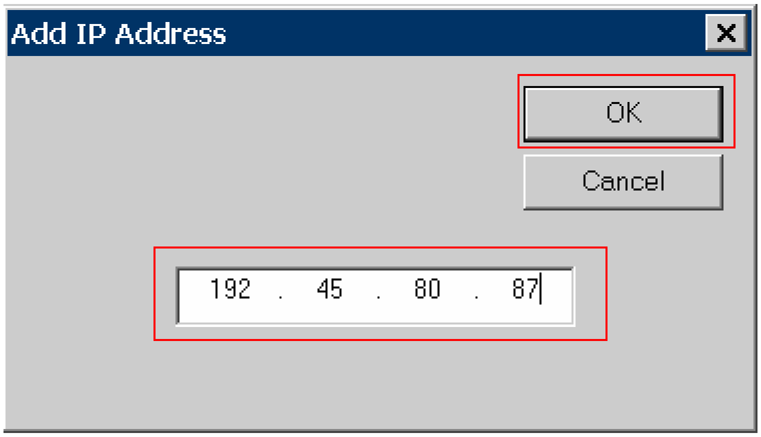
```
Listening on IP:192.168.1.50, Port:9000
MASTER THRD:Ready to Accept() connections
```

From the Site Number pulldown menu, select 0 - Local Site. For the IP Address, enter the IP address of the local site by selecting the **Add** button.



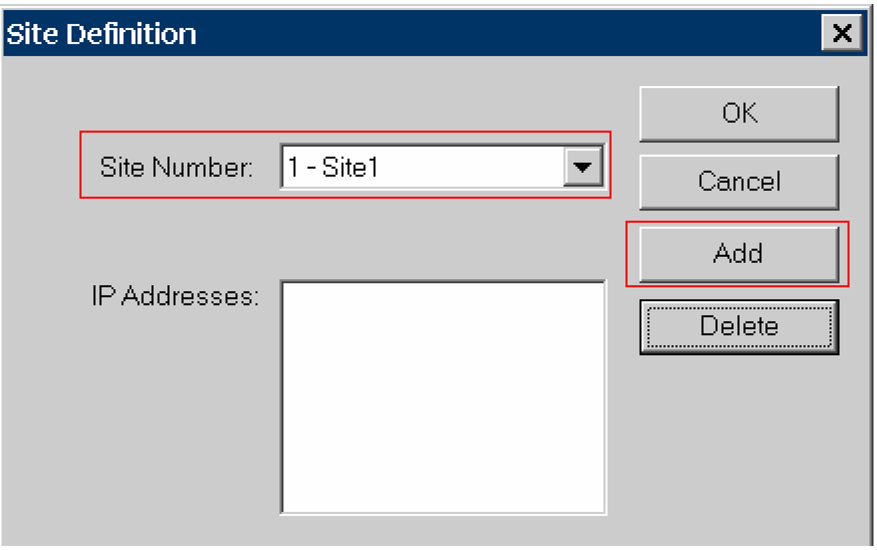
Site Number: 0 - Local Site

In the compliance test, this is the IP address of the Avaya S8700 Server which maps to node name “CLAN” in Avaya Communication Manager.
Select **OK**.



192 . 45 . 80 . 87

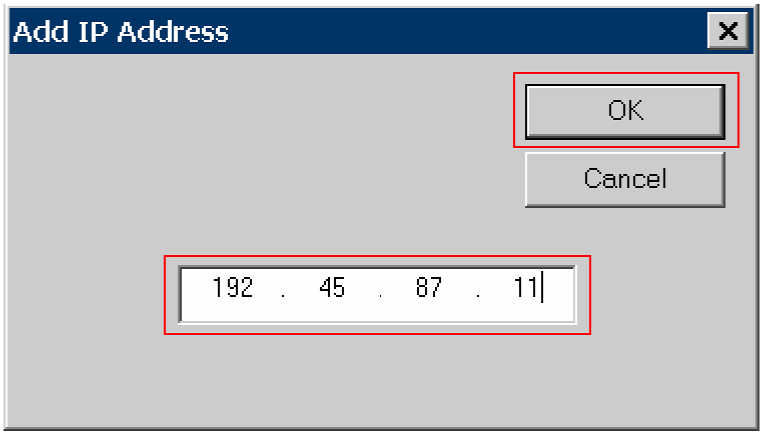
Repeat the previous step for the second site that was created. From the Site Number pulldown menu, select 1 – Site1. For the IP Address, enter the IP address of the site named Site1 by selecting the **Add** button.



Site Number: 1 - Site1

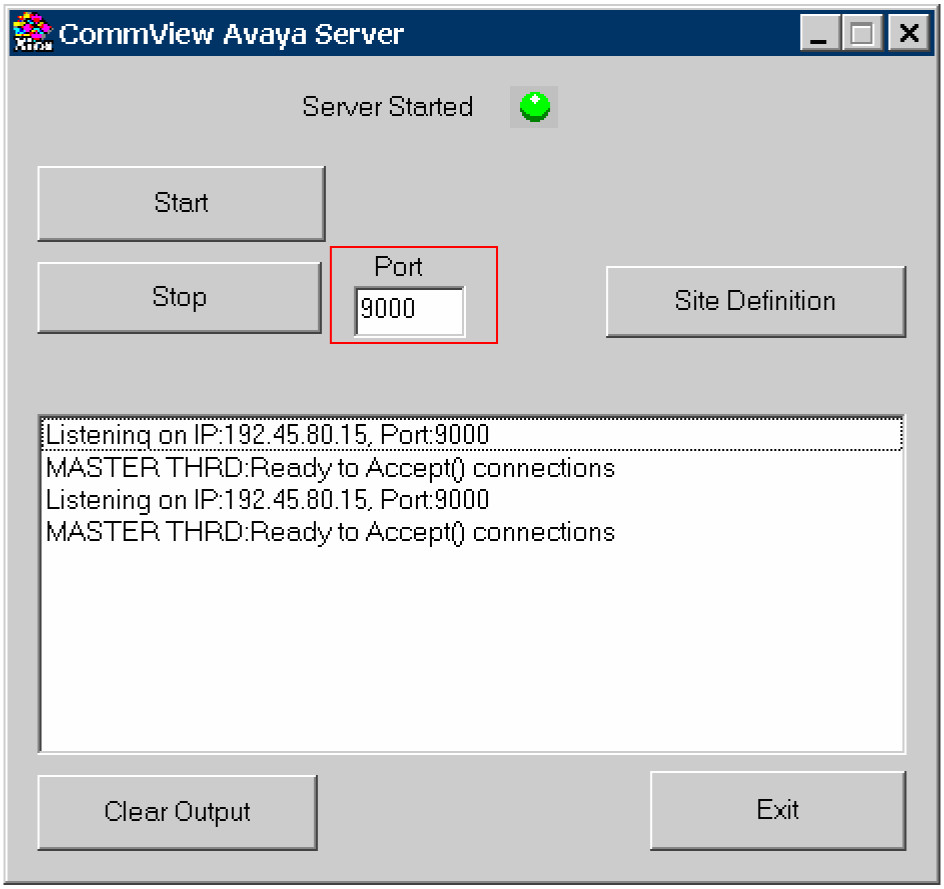
IP Addresses:

In the compliance test, this is the IP address of the procr interface in the Avaya S8300 Server that is connected to this network.
Select **OK**.



192 . 45 . 87 . 11

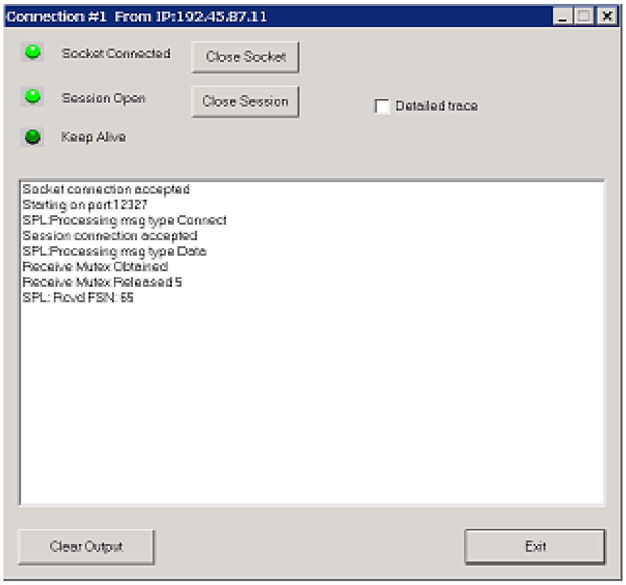
Set the port number to match the port number set on Avaya Communication Manager for use by the CDR link. Refer to Section 3. All sites must use the same port number. Click **Start**.



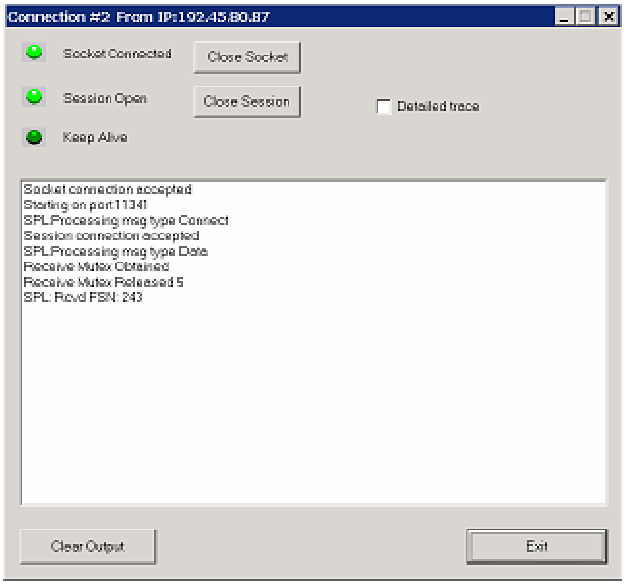
Port: 9000

```
Listening on IP:192.45.80.15, Port:9000
MASTER THRD:Ready to Accept() connections
Listening on IP:192.45.80.15, Port:9000
MASTER THRD:Ready to Accept() connections
```

The CommView Avaya Server will listen for connections from each site. The following window will appear for each site that has established a connection to the CommView Avaya Server. This window will remain open. Do not select **Exit**, otherwise the connection will drop.



```
Socket connection accepted
Starting on port 12327
SPL:Processing msg type Connect
Session connection accepted
SPL:Processing msg type Data
Receive Mutex Obtained
Receive Mutex Released 5
SPL: Rcvd FSN: 65
```



```
Socket connection accepted
Starting on port 11341
SPL:Processing msg type Connect
Session connection accepted
SPL:Processing msg type Data
Receive Mutex Obtained
Receive Mutex Released 5
SPL: Rcvd FSN: 243
```

5. Configure the Avaya LSP CDR Solution

This section describes how to configure the main Avaya Communication Manager and a LSP licensed Avaya Communication Manager to perform an Avaya LSP CDR solution. This section also includes the verification steps.

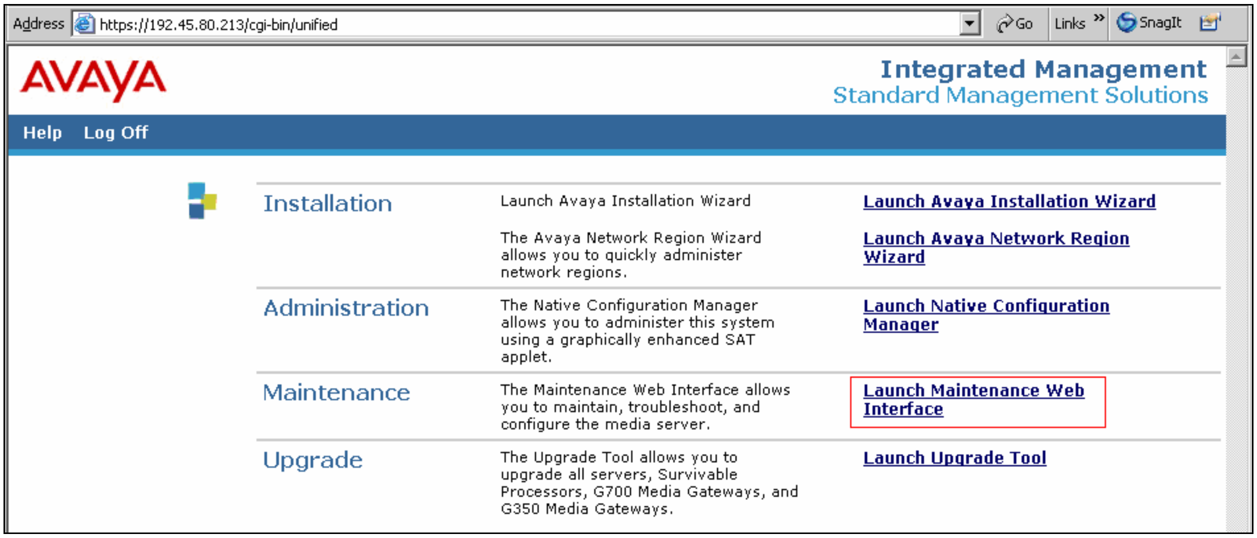
5.1. Configure Avaya S8700 Server (Main) with G650 Media Gateway for the Avaya LSP Solution

This section describes how to configure Avaya S8700 Server with G650 Media Gateway for the Avaya LSP CDR Solution. The following steps must be performed:

- Create member credentials (username/password) for a SFTP account
- Change “survivable-processor <assigned Survivable Processor node-name>” form
- Save the translation for LSP

5.1.1. CDR credentials for SFTP

To create credentials, enter https://<IP address of Avaya S8700 Server> in the URL, and log in with the appropriate credentials for accessing the Integrated Management Standard Management Solutions pages.
Select **Launch Maintenance Web Interface** link.


Address https://192.45.80.213/cgi-bin/unified
Go
Links
SnagIt
AVAYA
Integrated Management
Standard Management Solutions
Help
Log Off

Installation

Launch Avaya Installation Wizard — Launch Avaya Installation Wizard

The Avaya Network Region Wizard allows you to quickly administer network regions. — Launch Avaya Network Region Wizard

Administration

The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet. — Launch Native Configuration Manager

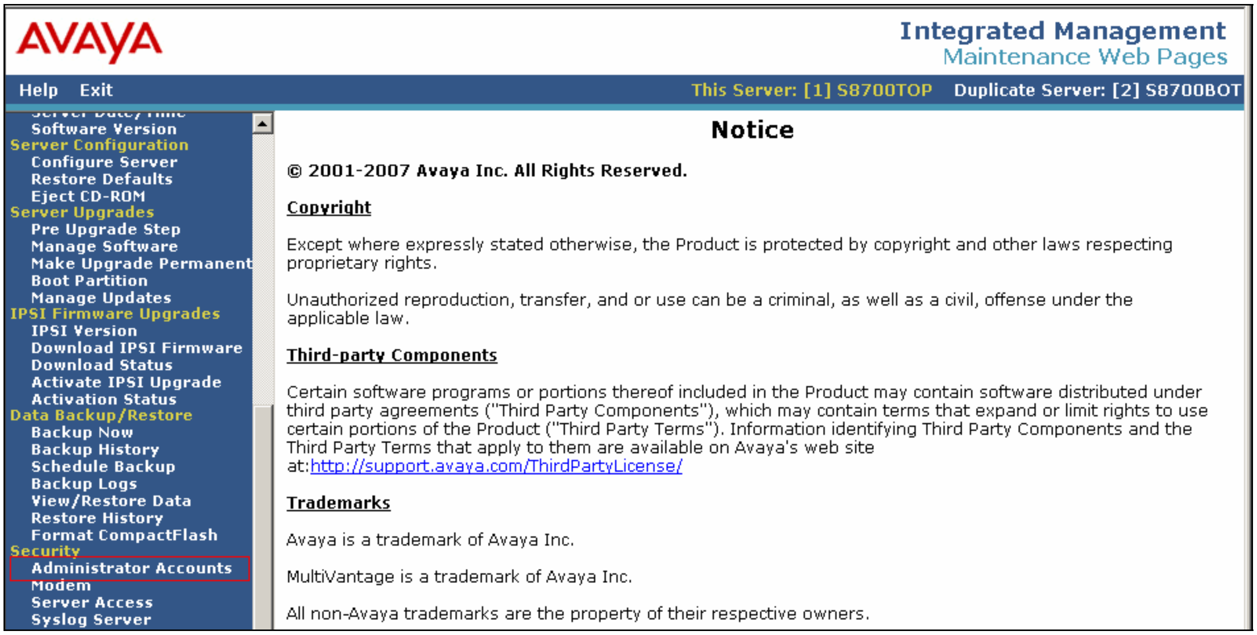
Maintenance

The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server. — Launch Maintenance Web Interface

Upgrade

The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways. — Launch Upgrade Tool

Select the **Administrator Accounts** link under the Security section.



Notice

© 2001-2007 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:http://support.avaya.com/ThirdPartyLicense/

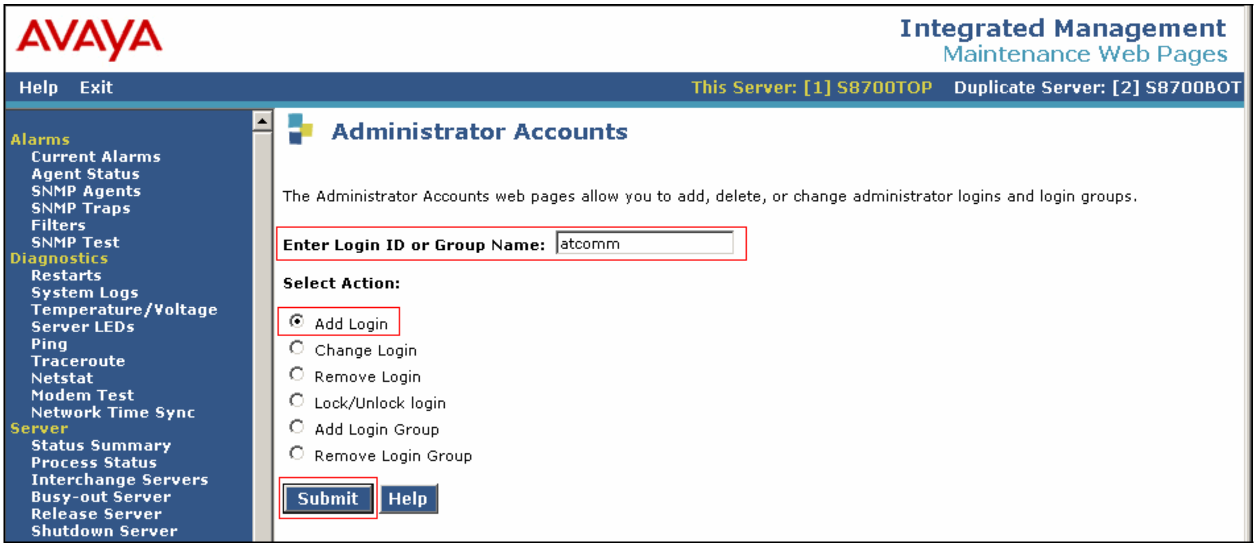
Trademarks

Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

In the Administrator Accounts page, provide a **Login ID** and click the **Add Login**.
Select **Submit**



Administrator Accounts

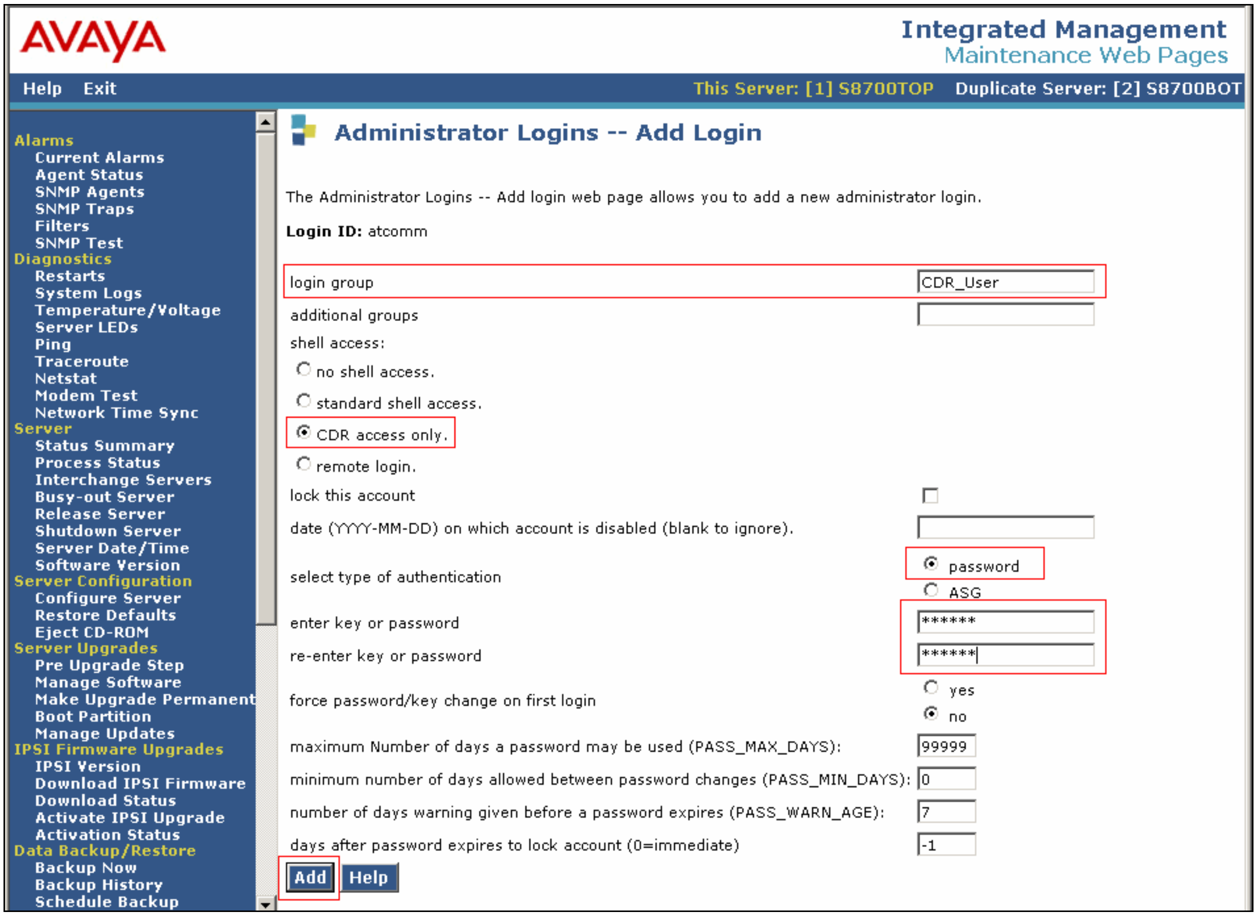
The Administrator Accounts web pages allow you to add, delete, or change administrator logins and login groups.

Enter Login ID or Group Name: atcomm

Select Action:

● Add Login
○ Change Login
○ Remove Login
○ Lock/Unlock login
○ Add Login Group
○ Remove Login Group

The CDR user has to be a part of the **CDR_User** group. Click the **CDR access only** for the shell access section. Click **Password** for the select type of Authentication field, and enter and reenter the password. Leave the default values for all other fields. Click Add.



Administrator Logins -- Add Login

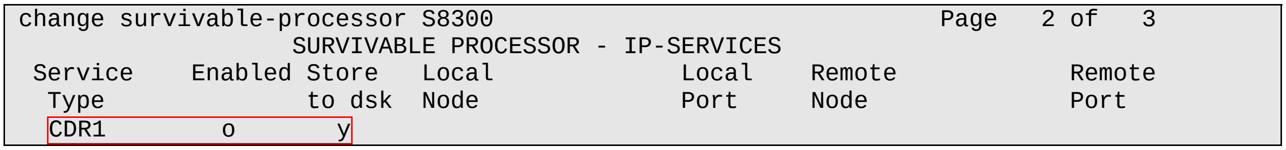
The Administrator Logins -- Add login web page allows you to add a new administrator login.

Login ID: atcomm

login group	CDR_User
additional groups	
shell access: ○ no shell access. ○ standard shell access. ● CDR access only. ○ remote login.	
lock this account	□
date (YYYY-MM-DD) on which account is disabled (blank to ignore).	
select type of authentication	● password ○ ASG
enter key or password	******
re-enter key or password	******
force password/key change on first login	○ yes ● no
maximum Number of days a password may be used (PASS_MAX_DAYS):	99999
minimum number of days allowed between password changes (PASS_MIN_DAYS):	0
number of days warning given before a password expires (PASS_WARN_AGE):	7
days after password expires to lock account (0=immediate)	-1

5.1.2. Survivable-Processor Form

Enter the **change survivable-processor S8300** command, where S8300 is an LSP licensed Avaya S8300 Server, configured in Section 3. Change the Enabled field to **o**, and the Store to dsk field to **y**.

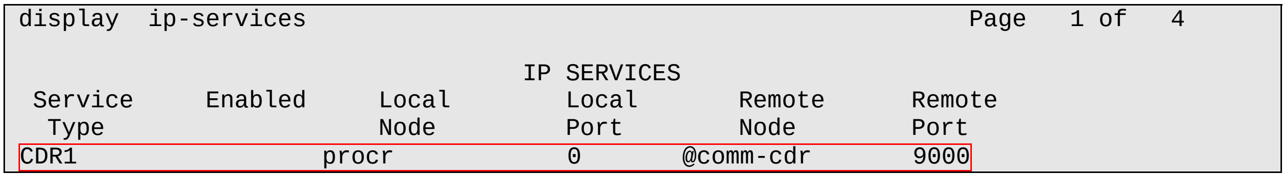


```
change survivable-processor S8300                              Page   2 of   3
                   SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local              Local    Remote            Remote
  Type              to dsk  Node               Port     Node              Port
  CDR1         o       y
```

After the Section 5.1.1 and 5.1.2 are completed, run the **save translation all** command, so that the translation in Avaya S8700 Server will be pushed to the LSP licensed Avaya S8300 Server.

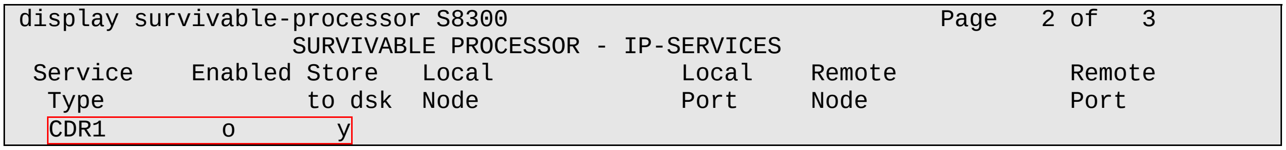
5.2. Verification from the Avaya S8300 Server for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the Avaya S8300 Server. Enter the **display ip-services** command. Notice that the Local Node field is changed to **procr**.



```
display  ip-services                                              Page   1 of   4


                                  IP SERVICES
 Service     Enabled     Local        Local        Remote      Remote
  Type                   Node         Port         Node        Port
CDR1                 procr            0       @comm-cdr       9000
```

Enter the **display survivable-processor S8300** command, and verify that the survivable-processor S8300 form in Avaya S8700 and S8300 Servers are identical.



```
display survivable-processor S8300                             Page   2 of   3
                   SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local              Local    Remote            Remote
  Type              to dsk  Node               Port     Node              Port
  CDR1         o       y
```

6. Interoperability Compliance Testing

The interoperability compliance testing included feature, serviceability, performance, and LSP testing. The feature testing evaluated the ability of the CommView CPE to collect and process CDR records for various types of calls. The serviceability testing introduced failure scenarios to see if the CommView CPE can resume CDR collection after failure recovery. The performance testing produced bulk call volumes to generate a substantial amount of CDR records. The Avaya LSP solution was tested by removing the CLAN board in the Avaya G650 Media Gateway.

6.1. General Test Approach

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Avaya Servers, and verify that the CommView CPE collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing, physical and logical links were disabled/re-enabled, Avaya Servers were reset and the CommView CPE was restarted. For performance testing, a call generator was used to place calls over an extended period of time. The LSP test was performed from the CommView using the SFTP command to the Avaya S8300 Server (LSP), and collecting the CDR records.

6.2. Test Results

All executed test cases passed. The CommView CPE successfully collected the CDR records from Avaya Communication Manager via a RSP connection for all types of calls generated including intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls. For serviceability testing, the CommView CPE was able to resume collecting CDR records after failure recovery including buffered CDR records for calls that were placed during the outages. Performance tests verified that the CommView CPE could collect call records during a sustained, high volume of calls.

The CommView CPE also successfully collected the CDR records from the Avaya S8300 Server using the SFTP command.

7. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of each Avaya Media Server, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that the CommView CPE received the CDR record for the call. Compare the values of data fields in the CDR record with the expected values and verify that the values match.
- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in the CommView CPE, and verify the report's accuracy.

8. Support

Technical support for the CommView CPE can be obtained by contacting @Comm via the support link at http://www.atcomm.com.

9. Conclusion

These Application Notes describe the procedures for configuring @Comm CommView CPE to collect call detail records from Avaya Communication Manager running on Avaya Servers. The CommView CPE successfully passed all compliance testing.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com .

[1] Feature Description and Implementation For Avaya Communication Manager, Release, Issue 5, February 2007, Document Number 555-245-205
[2] Administrator Guide for Avaya Communication Manager, Issue 3.1, February 2007, Document Number 03-300509

The following CommView CPE product documentation is available from @Comm. Visit http://www.atcomm.com for company and product information.
[3] CommView CPE Installation Guide

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.